Research Paper | Engineering | E-ISSN No : 2454-9916 | Volume : 4 | Issue : 3 | March 2018

AN EFFECTIVE APPROACH FOR PREVENTING INFERENCE ATTACKS IN CYBER SPACE

Shyamala J. [1] | Indu L. [1] | Thiyagarajan G. [1] | Shyam R. S. [1]

[1] Assistant Professor, Department of CSE, P. B. College of Engineering, Tamilnadu, India.

ABSTRACT

Web applications are now widely used for forecasting all kinds of information through a web page accessed via network . Its users habitually approach their websites by means of it's URL and unique domain name , all the sites in cyber space are provided with exclusive domain identity .In this context, URL shortening services are supervened that provide perpetual user easy and defended access, at first a short alias of a long URL for sharing it between trusted parties and also benefits easy remembrance and public click analytics mechanism of shortened URLs. The public click analytics is provided in an aggregated form to preserve the privacy of individual users. In this paper, we propose practical forestalling techniques to find inferring user's who clicks which shortened URLs on our web app. Unlike the conventional browser history stealing attacks, the forestalled attack demands private information without the knowledge of the user and will cause information security breach. Evaluation results show that this attack is more vulnerable when compared with the existing attacks thus we provide inference prevention mechanism for thwarting it.

KEY WORDS: URL shortening service, privacy leak, inference.

I. INTRODUCTION:

Data mining technology are increasingly used for analyzing data and storing large data sets along with this security integrated with it provides defended access. Large amounts of domain names, URL, approaching users data have been generated and collected at an unprecedented speed and scale. For example, the new generation of sequencing technologies enables the processing of hundreds of sequence data per day, and the application of web applications database is documenting large amounts of users data. security applications present new techniques to discover vulnerabilities and to acquire knowledge about it and create methods to improve the preventive measure for the information data preserved. The three major sub disciplines: at first URL shortening, then click analytics and inference prevention mechanism. Specifically, in URL shortening ,normal URL's are shortened which gives understanding complexity to new user and provides easy and defended access for authorized user, and with click analytics, from the vast amount of collected data's they are subjected to modules where authorized entry is compounded and given access. IPM is based upon the novel methodology implemented for thwarting inference attacks happening in cyber space.

Information security threats come in many different forms. Some of the most common threats today are software attacks, theft of intellectual property, identity theft, theft of equipment or information, sabotage, and information extortion. Data generated by users accessing web apps need to be collected and processed to provide in-depth knowledge. In this paper we propose new users details which are subjected to profiling monitoring and matching modules in order to provide authorized entry. We implement a IPM methodology which provides storage services to users credentials ,analytics of corresponding data to visualize and monitor secure information, physical activities performed by the users creating logins URL's for all accessible platforms. Our prototype system successfully integrates various technology platforms and provides thwarting for inference attacks.

II. RELATED WORKS:

2.1 Scriptless Timing Attacks on Web Browser Privacy:

A novel timing attack method to sniff users' browsing histories without executing any scripts. Our method is based on the fact that when a resource is loaded from the local cache, its rendering process should begin earlier than when it is loaded from a remote website. We leverage some Cascading Style Sheets (CSS)[1] features to indirectly monitor the rendering of the target resource. Three practical attack vectors are developed for different attack scenarios and applied to six popular desktop and mobile browsers. The evaluation shows that our method can effectively sniff users' browsing histories with very high precision. We believe that modern browsers protected by script-blocking techniques are still likely to suffer serious privacy leakage threats.

2.2 Privacy Risks of Collaborative Filtering:

Modern recommenders are based on collaborative filtering[2]; they use patterns learned from users' behavior to make recommendations, usually in the form of related-items lists. The scale and complexity of these systems, along with the fact that their outputs reveal only relationships between items (as opposed to information about users), may suggest that they pose no meaningful privacy risk.In this paper, we develop algorithms which take a moderate amount of auxiliary information about a customer and infer this customer's transactions from temporal changes in the public outputs of a recommender system. Our inference attacks are passive and can be carried out by any Internet user. We evaluate their feasibility using public data from popular websites Hunch, Last.fm, Library Thing, and Amazon.

2.3 De-Anonymizing Social Networks And Inferring Private Attributes Using Knowledge Graphs:

The users' identity information is always removed, attackers can still de-anonymize users with the help of auxiliary information. To protect against de-anonymization attack, various privacy protection techniques for social networks have been proposed. However, most existing approaches assume specific and restrict network structure as background knowledge and ignore semantic level prior belief of attackers, which are not always realistic in practice and do not apply to arbitrary privacy scenarios. Moreover, the privacy inference attack in the presence of se- mantic background knowledge is barely investigated. To address these shortcomings, in this work, we introduce knowledge graphs to explicitly express arbitrary prior belief of the attacker for any individual user. The processes of de-anonymization and privacy inference are accordingly formulated based on knowledge graphs. Our experiment on data of real social networks shows that knowledge graphs can strengthen de-anonymization and inference attacks, and thus increase the risk of privacy disclosure. This suggests the validity of knowledge graphs as a general effective model of attackers' background knowledge for social network privacy preservation.

III. SYSTEM ANALYSIS:

The Attackers tries to obtain the publicly available information of user. If they want to get a users data from twitter then twitter functionality is it has a tweet contains 140 characters. So user will perform the URL Shortening service to convey their message via spreading that URL to the concerned person. This service had been provided with some pre defined URL's to convey user message but that URL's are vulnerable as attackers could use it or save it in their database. So whenever user access their account the information can be stolen by attackers without the knowledge of users. And majorly this System fully based on twitter and attacks on twitter user.

The disadvantages are:

- Information security breach occurs
- Twitter does not officially provide personal information so personal information's are inferred without knowledge of user
- It's having length restriction
- Vulnerable to users
- No filtration of legitimate user's is done as all types of user's are given access

IV. SYSTEM DESIGN:

In the system we are integrating the Inference prevention mechanism With Mining of legitimate URL's. We propose a more secure system to provide the entry of an web application in more efficient way. The module phase allows only the authorized user to access our web application and details of that user is automatically updated into our Database by then periodic monitoring is done to take care of the frequent users accessing the web app by cross checking and verifying their

details with the existing and blacklisted entries followed by matching module if accessing entries leaves same traces of the blocked entries then that particular user will not be permitted for access into our web app.

The user can even know about the genuine search URL's by giving the domain names and this system also checks for legitimate search sites by checking these measures like authorized domain name and location replication. if location is replicated in approaching URL's then its blocked once and for all. All user information's are stored in respected database, particular user information can be modified or deleted only by an authorized person .the users didn't have to worry about the security breach from other login platforms as specialized login entries are given for shortlisted platforms where mischievous platform access into our web app is prohibited . the main advantage is that the user's web app will be forestalled from inference attacks and other security breach tactics.

The advantages are:

- We propose novel attack technique to prevent the users visiting history.
- it can increase the practicality of attacks so that we demand immediate counter measures to prevent.
- mining of legitimate search URL's can be found for any website given where red sites can be found
- sites with genuine domain name and location can be found avoiding illegal sites
- enables trusted entries by giving access to accepted persons entry and feedbacks can be given amongst that group for more intractability

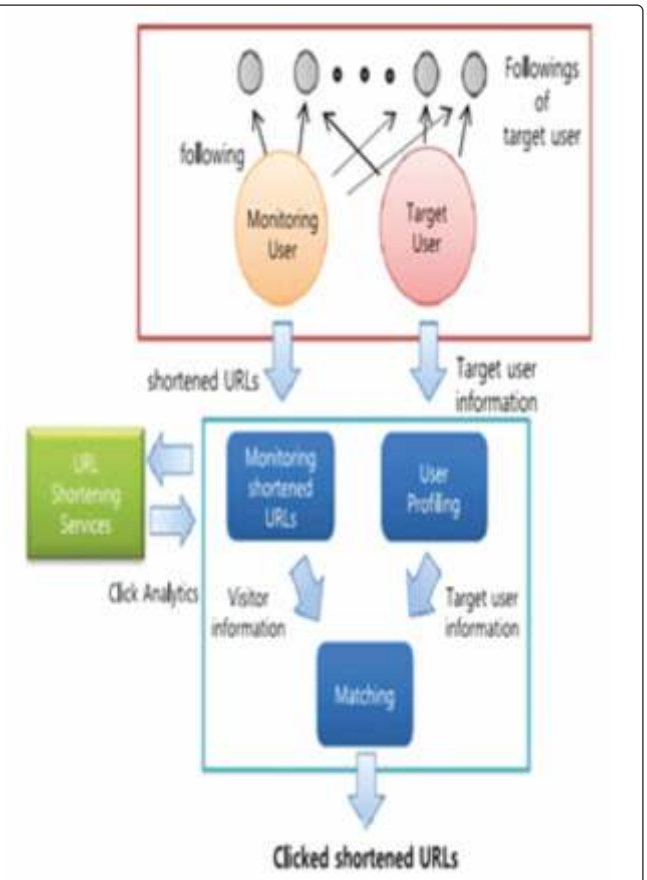

Fig 4.1: System Architecture

4.1 Profiling:

Data profiling utilizes methods of descriptive statistics such as minimum, maximum, mean, mode, percentile, standard deviation, frequency, variation, aggregates such as count and sum, and additional metadata information obtained during data profiling such as data type, length, discrete values, uniqueness, occurrence of null values, typical string patterns, and abstract type recognition. The metadata can then be used to discover problems such as illegal values, misspellings, missing values, varying value representation, and duplicates. Different analyses are performed for different structural levels. E.g. single columns could be profiled individually to get an understanding of frequency distribution of different values, type, and use of each column. Embedded value dependencies can be exposed in a cross-columns analysis. Finally, overlapping value sets possibly representing foreign key relationships between entities can be explored in an intertable analysis. Normally, purpose-built tools are used for data profiling to ease the process The computation complexity increases when going from single column, to single table, to cross-table structural profiling. Therefore, performance is an evaluation criterion for profiling tools.

4.2 Monitoring:

4.2.1 Privileged User Monitoring:

Monitoring privileged users, such as data base administrators (DBAs), developers, and outsourced personnel – who typically have unfettered access to corporate databases – is essential for protecting against both external and internal threats. Privileged user monitoring includes auditing all activities and transactions; identifying anomalous activities (such as viewing sensitive data, or creating new accounts with super user privileges); and reconciling observed activities (such as adding or deleting tables) with authorized change requests. Since most organizations are already protected at the perimeter level, indeed a major concern lies with the need to monitor and protect from privileged users. There is a high correlation therefore between database security and the need to protect from the insider threat. This is a complex task as most privileged users are capable of using sophisticated techniques to attack the database - stored procedures, triggers, views and obfuscated traffic - attacks that may be difficult to detect using traditional methods. In addition, since targeted attacks frequently result in attackers gaining privileged user credentials, monitoring of privileged activities is also an effective way to identify compromised systems.

As a result, auditors are now demanding monitoring of privileged users for security best practices as well as a wide range of regulations. Privileged user monitoring helps ensure:

- Data privacy, so that only authorized applications and users are viewing sensitive data.
- Data governance, so that critical database structures and values are not being changed outside of corporate change control procedures.

4.2.2 Cyber attack Protection:

SQL injection is a type of attack used to exploit bad coding practices in applications that use relational databases. The attacker uses the application to send a SQL statement that is composed from an application statement concatenated with an additional statement that the attacker introduces. Many application developers compose SQL statements by concatenating strings and do not use prepared statement; in this case the application is susceptible to a SQL injection attack. The technique transforms an application SQL statement from an innocent SQL call to a malicious call that can cause unauthorized access, deletion of data, or theft of information. One way that DAM can prevent SQL injection is by monitoring the application activity, generating a baseline of "normal behavior", and identifying an attack based on a divergence from normal SQL structures and normal sequences. Alternative approaches monitor the memory of the database, where both the database execution plan and the context of the SQL statements are visible, and based on policy can provide granular protection at the object level.

4.3 Matching:

Data matching can be done in order to discard duplicate content, or for various kinds of data mining. Many efforts at data matching are done for the purposes of identifying a key link between two data sets for marketing, security or other applied uses.

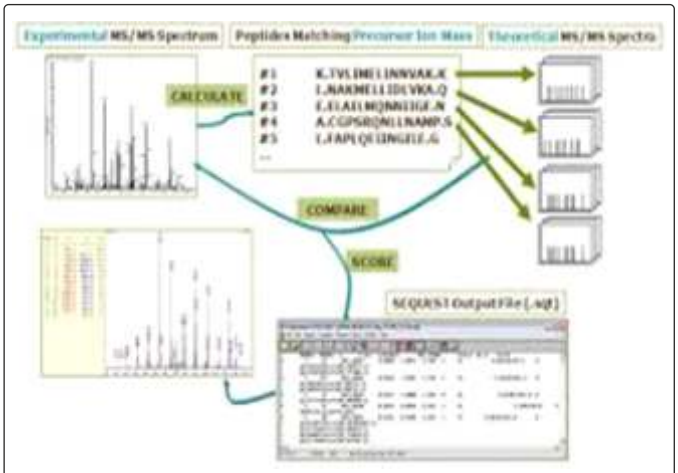

Fig 4.2: Data Matching

In general, data matching allows those holding large amounts of data to perform more precise searches that produce more efficient results. Some would argue that data matching capability can be used in ways that constitute a threat to personal privacy, especially where the use of diverse data sets is not explicit or transparent. Data matching may be one of the issues that gets added to the overall ongoing debate about personal privacy in an era .

V. CONCLUSION:

The implemented inference prevention mechanism is effectively administered in such a way that no type of unauthorized URL access is allowed in web application created the accuracy of this mechanism involves in subjecting the requesting user into three effective modules to grant only authorized entry. Thus as a future work from the pre processed review use of VPN's stands as a hurdle for identifying approaching user's browser platform and current location because VPN's acts virtually that could re identify all credentials like IP address and current location to overcome this IP address lookup can be used which will return the location of the VPN server as it cannot be faked .

REFERENCES:

1. A. Janc and L. Olejnik, "Web browser history detection as a real-world privacy threat," in Proc. 15th Eur. Conf. Res. Comput. Secur., 2010, pp. 215–231.
2. S. Krishnan and F. Monrose, "Dns prefetching and its privacy implications: When good things go bad," in Proc. 3rd USENIX Workshop Large-scale Exploits Emergent Threats, 2010, pp.10–10.
3. J. Lindamood, R. Heatherly, M. Kantarcioglu, and B. Thuraisingham, "Inferring private information using social network data," in Proc. 18th Int. World Wide Web Conf. (WWW), 2009.
4. A. Mislove, B. Viswanath, K. P. Gummadi, and P. Druschel, "You are who you know: Inferring user profiles in online social networks," in Proc. 3rd ACM Int. Conf. Web Search and Data Mining, 2010, pp. 251–260.
5. A. Narayanan and V. Shmatikov, "Robust de-anonymization of large sparse data set," in Proc. IEEE Symp. Secur. Privacy, 2008,
6. J. Song, S. Lee, and J. Kim, "I know the shortened urls you clicked on twitter: Inference attack using public click analytics and twitter metadata," in Proc. 22nd Int. World Wide Web Conf., 2013, pp. 1191– 1200.
7. Z. Weinberg, E. Y. Chen, P. R. Jayaraman, and C. Jackson, "I still know what you visited last summer: Leaking browsing history via user interaction and side channel attacks," in Proc. IEEE Symp. Secur. Privacy, 2011, pp. 147–161.
8. G. Wondracek, T. Holz, E. Kirda, and C. Kruegel, "A practical attack to de-anonymize social network users," in Proc. IEEE Symp. Secur. Privacy, 2010, pp. 223–238.
9. E. Zheleva and L. Getoor, "To join or not to join: The illusion of privacy in social networks with mixed public and private user profiles," in Proc. 18th Int. World Wide Web Conf., 2009.